ABSTRACT

A network interface for secure virtual interface data communication includes a doorbell circuit, a processor, memory, and a bridge circuit. The doorbell circuit responds to physical I/O addresses of the host that are mapped by a memory management unit by a registration process. An application program seeking to use a channel of a virtual interface must register the virtual address of host memory where data for communication is or will be stored and register the virtual address of a page of I/O addresses. Access to the doorbell functions and to the host memory via the memory management unit are therefore denied when the requesting process identifier does not successfully compare with the process identifier for the process that performed the registrations. A password may be stored in the network interface in association with a virtual interface (VI) channel identifier and stored in association with the virtual to physical map used for VI communication. The network interface may abandon a requested or implied data communication function when passwords so not successfully compare. Methods for virtual interface (VI) communication performed by an application program may include one or more of the steps of (a) establishing a VI channel where physical I/O addresses of a network controller are secured; (b) registering host memory for use with a VI channel where physical memory addresses are secured; (c) describing blocks of host memory with reference to a memory handle; and (d) accomplishing data communication of a described block of host memory via an established VI channel where the data and controls of the VI channel are secured and the data and controls of other VI channels are secured. Security is provided against both erroneous operations and operations intentionally effected by rouge processes.